NIDS 防衛研究所 National Institute for Defense Studies
NIDSコメンタリー
第 399 号　2025 年 9 月 26 日

能動的サイバー防御の実装に向けた残された論点（後編）

――オペレーションの評価と戦略的コミュニケーションの必要性

政策研究部サイバー安全保障研究室　特任研究員　佐々木　勇人

はじめに

「前編」では 2022 年の国家安全保障戦略で示された能動的サイバー防御の 3 本柱（(ア）情報共有等の官民連携、(イ）通信情報分析、(ウ）アクセス・無害化）のうち、(イ）通信情報分析、(ウ）アクセス・無害化をめぐる法的論点について考察しながら、対抗オペレーションを実行するために必要な「ポートフォリオ」の概念と、ポートフォリオ分析に必要な（ア）情報共有等の官民連携について考察を進めてきた。「後編」では、能動的サイバー防御における対抗オペレーション実施後の「評価」について考察し、この観点においても「ポートフォリオ」分析とそのための「官民連携」が重要である点とともに、「戦略的コミュニケーション」が必要となる点について考察する。

対抗オペレーションは「評価」することが可能なのか

能動的サイバー防御の関連法・整備を巡って、本稿前編にて紹介のとおり、通信情報分析などのプロセスの不透明性への指摘がある。そもそも公的組織が実施するサイバー空間上の活動のほとんどは「攻撃者側に知られる恐れがあるので詳細は差し控える」[1]というスタンスのものが多いが、さらに Offensive なサイバー作戦はその性質上、秘密裏に実施されることが多い。秘密裏に実施されることの問題点は、よく指摘されるような①政府の活動の透明性の論点のほか、②オペレーションの運用保全を過度に意識した秘密主義に陥るリスク、③各対抗オペレーションの評価が適切に行えない問題、④能動的サイバー防御全体の成果を不十分にする恐れ、の 4 点があると筆者は考える。(①、②については本稿の主たるテーマ

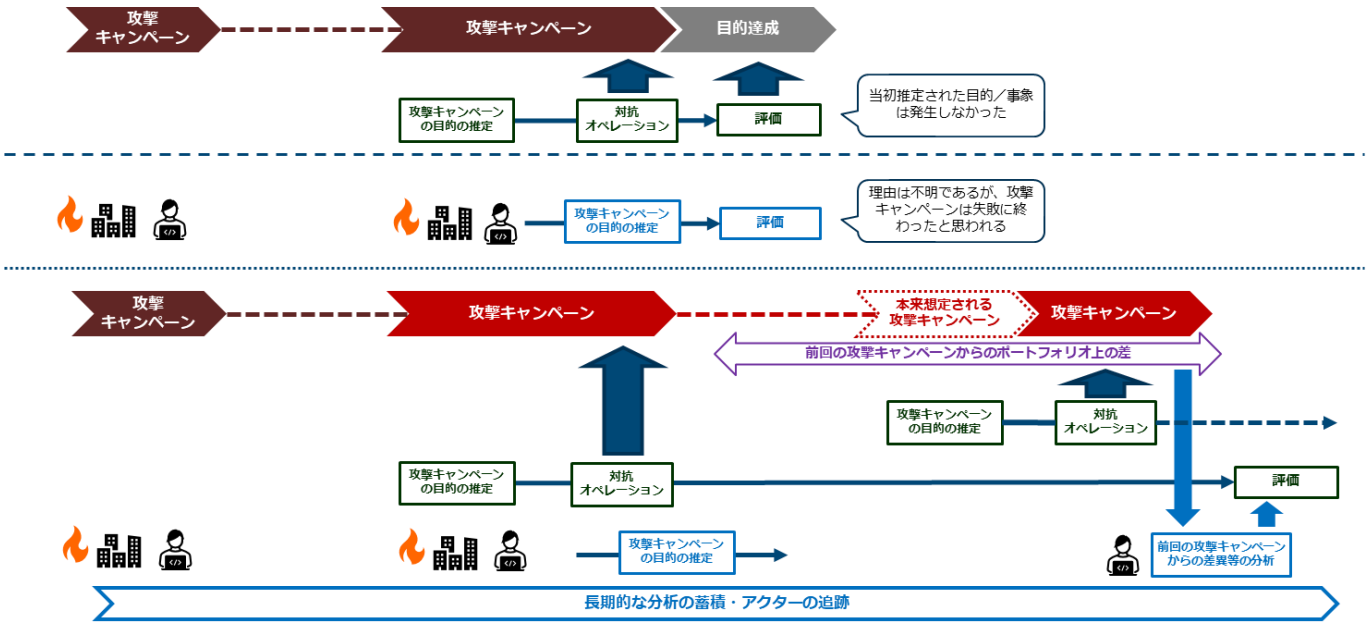
ではないことや既に先行研究もあることから省略する）

まず③についてであるが、個別の対抗オペレーションが対象とする攻撃キャンペーンに与えた効果をどのように評価することができるのか考えてみたい。対抗オペレーションの効果は、これまでのコメンタリー[2]で考察の通り、Ａ：攻撃キャンペーンを中断させ相手方の目的を未達に終わらせること、Ｂ：対抗キャンペーンの繰り返しにより累積的ダメージを与えること（ポートフォリオへの影響、継戦能力への影響）、Ｃ：相手方の意思決定への影響、の大きく 3 つにある。A の評価は比較的シンプルであり、攻撃キャンペーンの目的と推測された事象（例：重要インフラシステムの破壊、国の重要イベントの妨害／介入）が発生しなかったことで評価することが可能なケースがある（例：VoltTyphoon に関する 2025 年 7 月の米当局者の見解等（後述の表 1 参照））。

他方で、B、C については、長期にわたる攻撃キャンペーンの繰り返しの観測において、攻撃キャンペーン間の期間の変動やＴＴＰの変化など、その評価点、変数は多岐にわたるため、前述の通り、特定アクターの活動を追跡する多くのセキュリティ専門組織の知見・見解を相互に参照しながら分析しなければならない。特に対抗オペレーションにとって必須であるポートフォリオ分析については前編にて考察の通り、その長期的な分析・追跡において行政機関での対応は難しく、基本的に民間の専門知見の力を借りるほかない。

下記図下段の通り、ポートフォリオへの打撃効果の測定ができるのは、対抗オペレーションの対象となった攻撃キャンペーンではなく、その次の攻撃キャンペーンの後である。対抗オペレーションを実施したこと自体が完全に秘匿された場合、この事情を知らない民間専門組織の多くは攻撃キャンペーン間の変化の原因を別の要因に求めることになるため、対抗オペレーションで攻撃者側に変化が起こったかどうか検証がなされないことになるのである。

図：攻撃キャンペーンのサイクルと対抗オペレーションの評価サイクルとのズレの関係



対抗オペレーションにおける「勝利」とは何か

前述の「④能動的サイバー防御全体の成果を不十分にする恐れ」の論点について、そもそも対抗オペレーションにおける「勝利」とは何かという視点から考察してみたい。別の拙稿[3]にて、対抗オペレーションにおける「勝利」とは何かについて考察を行った。対抗オペレーションもまた攻撃キャンペーンと同じく、武力行使未満の活動で実施されるため、また、前編で考察の通り、基本的には相手方への「累積的効果」を狙うため、“長い闘い”にならざるを得ない。ややもすると、「消耗戦」の様相を呈するかのように見える対抗オペレーションは、どのような形で「勝利」を得ることができるのだろうか。

対抗オペレーションの「勝利」について、軍事戦略における「勝利」を評価する 4 つの観点（①目標ベースでの「勝利」の評価、②費用対効果ベースの「勝利」の評価、③観念ベースの「勝利」の評価、④規範ベースの「勝利」の評価）[4]からの考察を行った（下記図参照）。各観点の解説については前述の拙稿をご参照いただきたい。

表：サイバー対抗オペレーションの「勝利」を評価するための 4 つの視点

	目標ベース	費用対効果ベース	観念ベース	規範ベース
「勝利」の	目標達成状態に達	政治的目標達成状態に	勝利の概念は社会的	戦いながら紛争当事者

評価	すると勝利を宣言し、達成できなければ敗北であると考えるもの。	達することを、そのためにかかった費用と比較して評価すること。	に構築・「創造」されるものであり、戦争とは何かという一連の先入観、価値観、軍事行動への期待値、そしていかに情報が処理され拡散するかに影響を受けるとするもの	それぞれの「規範」がさらけ出され、規範構造を「共有」することにより、共同規範構造が形成され、勝利が理解される／相手に理解させるというもの。
事例	Volt Typhoon への対処[5]や、2022 年ウクライナ侵攻前後の攻撃キャンペーンに対する米・ウクライナの Hunt Forward オペレーション	－	（左記の「目標ベース」視点では攻撃は失敗に終わったと評価されるが、他方で）2024 年 12 月の米中当局者間の会合の場で、中国側から Volt Typhoon の攻撃活動を認めるような発言があり、米側参加者は台湾問題に絡んで米国に対して警告しているものと解釈したとされる。	ロシア側の攻撃実行者（GRU Unit 74455）が軍事活動として行う攻撃キャンペーンと、それに対する米側の対抗オペレーションや対抗措置のルール（刑事手続き、経済制裁指定）の食い違い
課題	関連損失を考慮しないまま戦争が進行することで目的達成状態が修正・変更され、「終わりの見えない展開」になるという問題点がある	費用便益計算の観点から勝利と敗北を理解する場合、価値観の対立に直面するという問題点がある	当初の攻撃目的が達成されなくても、脅迫効果／接近拒否的な使い方ができるというケース（上記）があり、攻撃キャンペーンの解釈によって、勝利／敗北が定められないケースである	（上記の通り、ルールの食い違いが発生する場合がある）

国家安全保障戦略では、「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」と示されており、前編にて解説の通り、政府としても「攻撃キャンペーン」単位で対処方針等を検討していく旨が示されているところ、上記の「勝利」を評価する 4 つの視点で挙げたところの、「①目標ベースでの「勝利」の評

価」が一番近いのではないかと考えられる。ただ、軍事戦略において「勝利」の定義が定まらず、前述の４つの視点それぞれから評価がなされ得る点を踏まえると、対抗オペレーションの「勝利」を評価するためには、4 つの視点のどれか一つで足るものではなく、4 つそれぞれの視点から評価する必要があると筆者は考えている。

仮に何らかの事情により、対抗オペレーションを秘密裏に実施した場合、冒頭に触れた、対抗オペレーションの「勝利」における 4 つの観点の整理では、「目標ベース」のみで評価することになる。先述の通り、「目標ベース」だけでの評価は不十分であり、単なる「消耗戦」に陥る可能性が高い。さらに言えば、前項で解説の通り、オペレーションの効果測定もままならない。攻撃キャンペーンを秘密裏に不成功に終わらせるだけでは不十分であり、「勝利」における他の観点も踏まえて、戦略オーディエンスに向けた戦略コミュニケーションが必要になると筆者は考えており、その背景等について次項にてケーススタディも交えて考察する。

戦略的コミュニケーションの必要性

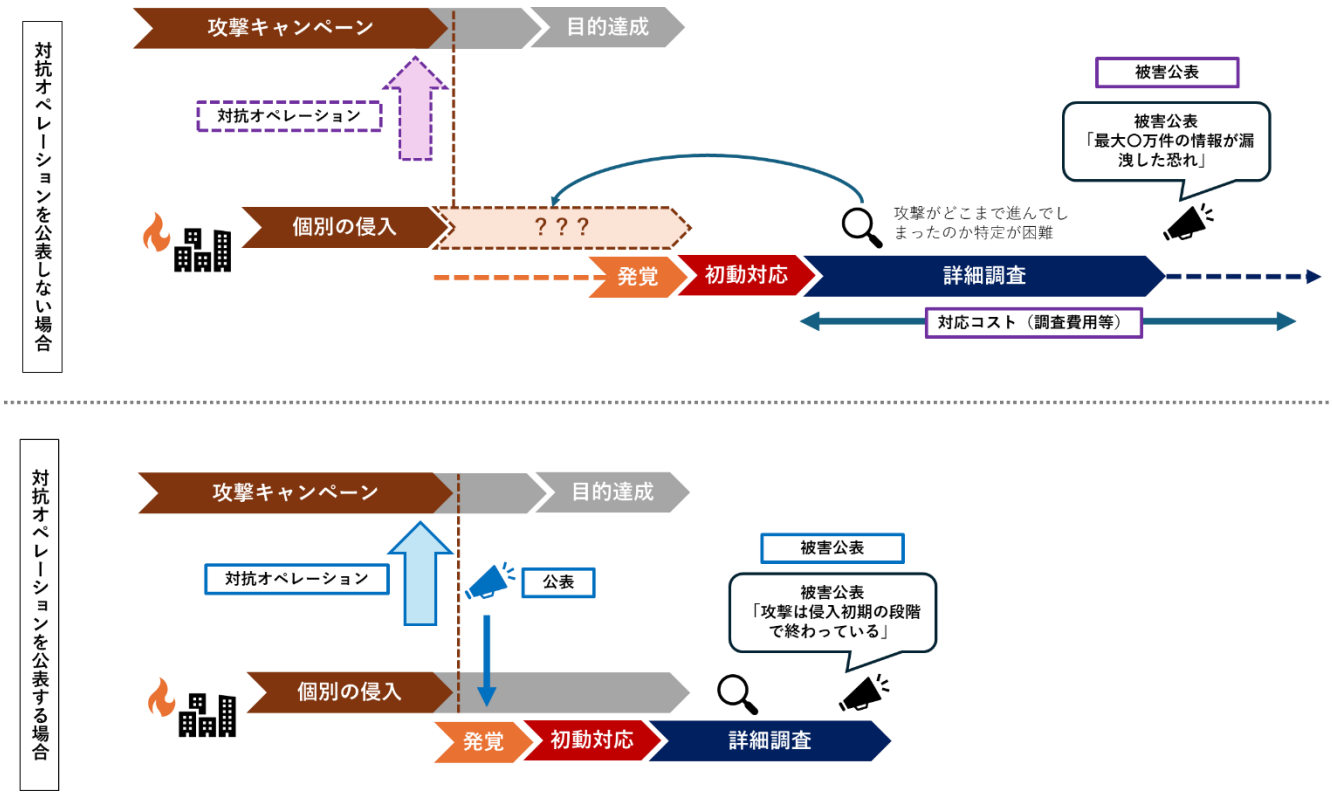
2025 年 7 月に Microsoft 社の Sharepoint の脆弱性が悪用される事案が発生し、100 組織以上が侵害され、米国家核安全保障局（NNSA）も被害にあったと報道がなされた。他方で、Micorosoft 側は攻撃活動に関するレポート（アクター推定や TTP 等）を公表した際に、そのタイトルを「Disrupting active exploitation of on-premises SharePoint vulnerabilities」[6]として発表したのである（※下線部は筆者）。この攻撃では複数のアクターが当該脆弱性を悪用していたことが判明しており、１つのアクターは過去にランサムウェア攻撃を行っていたアクターであることが判明しているほか、2 つの APT アクターについては初期アクセス（Initial Access）の開拓フェーズにとどまっていた可能性が示唆されており、この点からは比較的早期に「迎撃」できたと評することも可能である。

APT のような高度な攻撃活動ほど、個別の被害現場においては、攻撃者側の痕跡消去、攪乱、解析妨害等により被害の全容が判明しないことが多い。例えば、エスピオナージを目的とした攻撃の場合、結局どのような情報がどの程度窃取されたのか推定できないまま調査を終えざるを得ないケースが多い。他方で、複数被害事案を束ねた、攻撃キャンペーン全体の分析においては、攻撃者側の目的がある程度推定できる場合がある。個別の被害現場の調査だけではなく、マクロな観点での攻撃キャンペーン分析から逆に個別被害（攻撃目的が達成されたのか否か）の推定ができる場合があるのである。先述のような、広範囲な初期アクセス開拓の攻撃キャンペーンにおいては、個別被害では「ネットワーク境界面を侵害され

たのち、さらにネットワーク奥深くまで侵害されたのかどうか」疑問が出るわけであるが、追加調査コスト負担をどうするかという点で悩むとともに、そもそも攻撃者が痕跡を消していた場合、調査しても見つからない可能性など、多くの壁にぶつかることになる。他方で、複数被害現場の情報がまとまった、マクロな視点での攻撃キャンペーン分析情報を得ることで、自組織に対する攻撃がどこまで行われた可能性があるのか推測し、追加調査を行うのかどうか、被害の蓋然性などについて判断することが可能になるのである。

当該攻撃キャンペーンを先に紹介した報道の通り、「100 組織も侵害され、安全保障上の重要な組織まで侵害された」と捉えるのか、「攻撃キャンペーンを初期の段階で認知し、対処できた」と捉えるのかは大きな違いである。これは単に「社会全体の認識」というマクロなレベルの視点だけでなく、上記の通り、ミクロな個別被害対応／被害認知においても大きな影響を及ぼすものである。ここまで紹介したケースは対抗オプションの中でも比較的ソフトな「情報発信（注意喚起、インディケータ展開）」が用いられたケースであるが、アクセス・無害化のようなより強力が対抗オプションを用いたオペレーションにおいても、「アクセス・無害化実施によって、攻撃キャンペーン全体がどのフェーズで中断することができたのか」を示すことには変わりない。「②費用対効果ベースの「勝利」の評価」という観点については別の拙稿にて解説の通り、そもそも「被害とは何か」という制度上の定義の課題があるものの、個別の被害組織やこれを被害公表や報道等で認知する社会全体の被害認識に大きな影響を与えることになると筆者は考える。

図：対抗オペレーションの公表有無と個別の被害判定との関係

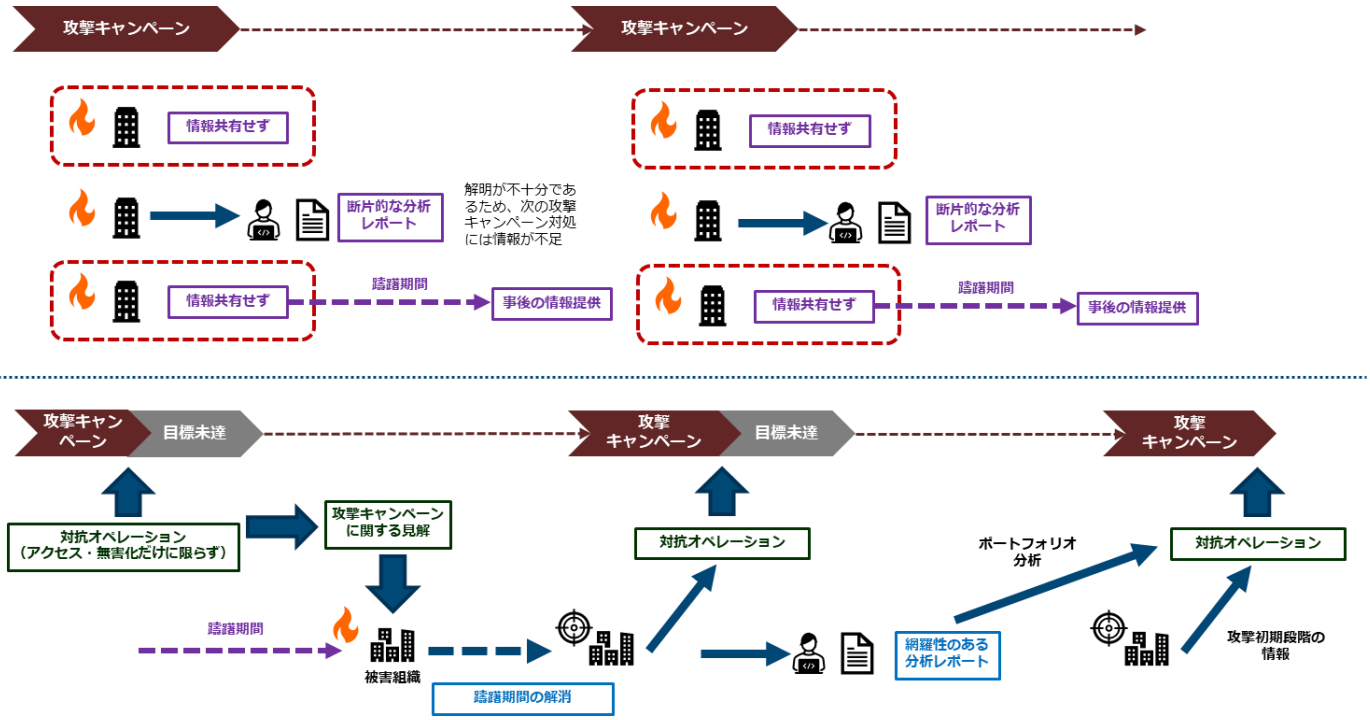


こうした、攻撃キャンペーン全体に関する情報発信はいわゆる「戦略的コミュニケーション」として、社会的レジリエンスを保つ効果を得ることができると考える。この点は脅威情報流通の観点からも重要である。統計的な情報がないため、あくまで筆者の本務先でのインシデント対応経験に基づくものであるが、高度なアクターによる攻撃で機微な情報が窃取された可能性が想定されたり、大量の個人情報漏えいの可能性が想定される事案ほど、外部への情報共有（提供）どころか、外部機関との接触自体にも慎重になる傾向が強い。これは技術的な問題というよりも推定される被害の（対外的な）インパクトを念頭に、レピュテーションリスクを踏まえて、コントロールされた情報開示（プレスリリース）前に被害事実が外部に知られることへの（特に経営層や管理部門の）拒否感が背景にある。現状の情報共有がうまく行われない原因の一つでもあるが、こと能動的サイバー防御の推進においては、こうした被害現場側の躊躇による脅威情報の流通不足は対抗オペレーション実施の根本を崩すことになる。

こうした躊躇はある程度調査が完了して、例えば「当初想定したような被害ではなかった」ことが判明したり、あるいは攻撃キャンペーン後に公開されたセキュリティ専門組織のレポートからおおよその被害規模が判明／推定できたタイミングで終了することが多い。他方でこのタイミングでは既に攻撃キャンペーンも終わっており、また、調査も（当該被害組織と調査ベンダが考える範囲では）終了してしまっているため、外部に相談／情報共有を通じて情報の照会をかけるインセンティブをすでに喪失していることから、やはり外部連携を通じた情報共有が行われないのである。

「鶏が先か、卵が先か」であるが、対抗オペレーションに関する（早期の）情報発信が行われることで、個別の被害組織が被害状況をこれまで以上に認識できるようになり、こうした「被害が判定できないことによる対外情報連携の躊躇期間」を低減させることができ、社会全体でより早期に脅威情報が流通するようになるのではないかと考える。

図：情報提供／共有までの「躊躇期間」の解消と対抗オペレーションのサイクルとの関係



さいごに

ここまで考察の通り、アクセス・無害化措置を含む対抗オペレーションの実施や通信情報分析に係る法制度等に係る論点については、「攻撃キャンペーン単位で対処すること」「攻撃者側のポートフォリオ分析に基づいてハード／ソフト様々な対抗オプションを組み合わせて対抗オペレーションを行うこと」によって解決することが可能と考えている。そして、能動的サイバー防御の取り組み全体として、アクセス・無害化措置をはじめとしたさまざまな対抗オプションと、通信情報分析や民間からのこれまで以上の情報共有をうまく組み合わせ、対抗オペレーションを成功させていくためには、長期に渡りアクター／攻撃キャンペーンを分析・追跡し、そのポートフォリオを分析・追跡する民間の専門知見を活用するこ

とと、対抗オペレーションに関する情報発信（戦略的コミュニケーション）が必要となる。

これを阻害する要因は「秘密性」にある。ここまでに述べた通り、対抗オペレーションを秘密裏に実施してしまえば、効果測定もできず、効果的なさらなるオペレーションの実施も難しい。また、戦略的コミュニケーションや、対抗オプションとしての情報発信も制限されるようになれば、「勝利」の見えない戦いになるのである。さいごに、この「秘密」の観点について若干の考察を捕捉したい。

サイバーセキュリティの世界では脅威インテリジェンス情報の大半が民間市場を通じて流通しており、扱われるデジタルデータの情報の特性からも、基本的に情報が流通・拡散するものとして扱われている。これは従前の（非サイバーセキュリティの）安全保障・インテリジェンスの世界を支えてきた伝統的なルールとは大きく異なる世界[7]である。サイバーセキュリティにおける情報流通の“力学”と、安全保障・インテリジェンスの世界を支えてきた伝統的なルールとの間のギャップが影響するのはいわゆる脅威インテリジェンスをめぐる官民間の情報共有だけの問題[8]ではない。先述の通り、対抗オペレーションに係る情報発信（戦略的コミュニケーション）という対抗手段実施においてもまた、同じギャップにぶつかることになるだろう。

サイバー攻撃、特に安全保障に影響を及ぼすようなエスピオナージや情報工作目的の攻撃活動について、「サイバー攻撃」を手段として用いることの有利な点はその「秘密性」ではなく、「スケーラビリティ」[9]であるが、その規模を広くするほど秘密性は失われてしまうことになる。ではなぜ、広範囲に実施される APT キャンペーンに対して攻撃者側に負けている／後追いになってしまっているのかと言えば、防御側が連携できていないためである。被害組織間、商用セキュリティ製品・サービス間、官民間にそれぞれ脅威情報の共有ギャップがあり、いわばこうした防御側の「分断」がある以上、攻撃者はスケーラビリティの利点を最大限受益して累積効果を生んでいるのである。こうした防御側の各プレイヤー間の「分断」には様々な論点・課題があるが、能動的サイバー防御の能力整備の観点からは、我が国におけるサイバーセキュリティ対処能力の構築において、米国のような強力なインテリジェンス能力がただちに得られない以上、官民の隔たりを超えて、行政側は民間（専門家）の脅威情報流通に入り、これを最大限活用することが重要であると筆者は考える。

もう一点、戦略／ドクトリンの論点についても付記しておきたい。筆者が研究対象としている、サイバー攻撃への対抗オペレーションの「ドクトリン」について、「戦略やドクトリンは相手に知られてはならないので、公開すべきではない」という意見をよく耳にする。この戦略（あるいはドクトリン）の秘匿可否の論点について、Ｊ・Ｃワイリーの以下の言及[10]が重要であると考える

> 戦略そのものには全く「秘密」などというものはない、ということだ。「戦略の研究は門外不出だったために、今まで誰も研究を行うことができなかった」ということが、全く根拠もないまましつこく言われ続けている。ただしこれは、敵に対して自分たちが今これから特定の状況の中で一体何を行おうとしているのか全部教えても全然平気だ、ということを意味しているわけではない。もしこれが本当だとしたら、それは単なる愚かな行為である。しかし、だからといってそれが（意識的、そして多くの場合は無意識的に戦略思想家に影響を及ぼすような）外部からのアイデアの流入を極力避けるべきだ、ということにもならない。実際はむしろその逆であり、このような閉鎖的な知的活動はいわば「知的近親相姦」になるだけであり、平凡で無能な戦略へと質の低下を招くだけなのだ。お互いに批判することもなく内輪で褒めあいながら行う知的活動も楽しいものなのかもしれないが、これが知的活動の向上にはつながらない。よって、戦略的思考の基本的パターンというのは何か秘密のものとして考えられるべきではない。このようなパターンを多くの人々が理解すればするほど、戦略的決断を行う際の我々の民主制度が健全になるのだ。（略）

前述の通り、秘密裏に行う対抗オペレーションで攻撃キャンペーンを失敗に終わらせたとしても、確かに「安全」は保たれたかもしれないが、被害／標的組織やその他の多くの組織／人々は「安心」を感じることはないだろう。そして、秘密裏に行っている作戦の実態と、国が公に示す情報が矛盾するようなことになれば、戦略的コミュニケーションは破綻[11]し、サイバー攻撃に対する社会全体のレジリエンスは維持されず、いくら対抗オペレーションをやったところで、社会として敗北感／虚無感がただ広がるばかりとなるだろう。なにも、個別事象の対処経緯をすべてさらけ出せということではなく、総論として、どのような戦略／ドクトリンに基づいて対処がなされるのかを社会に対して事前に示すことは可能である。

民間の専門家コミュニティや被害／標的組織から速やかな情報提供を得るためにも、また、同盟国をはじめ海外からの情報を得るためにも、新体制においてどれだけ戦略／ドクトリンを示せるかが、能力整備の第一歩であり、また、それ自体が攻撃者対処のための戦略的コミュニケーションの第一弾となるであろう。いかに戦略／ドクトリンが示せるかが、能動的サイバー防御における新組織体制の重要な試金石となると筆者は考えている。

[1] この「秘密性」の議論については、実務ベースの議論が見受けられないが、例えばサイバーセキュリティ専門のネットメディア「The Record」の Alexander Martin はジャーナリストの Kim Zetter らとの対談にて「すべてを完全に秘密裏に行う必要はない。ある程度、一部の能力は敵対勢力に晒されている」と指摘している。（Alexander Martin, Joe Tidy, Kim Zetter, Joe Devanny and Tim Stevens, “Reporting on cyberwarfare: a conversation”, RESERCH HANDBOOK ON Cyberwarfare（Edward Elgar Publishing, 2024）収録）

[2] 本稿前編及び、NIDS コメンタリー　第 346 号　2024 年 8 月 6 日（特集：「新領域の安全保障」 vol.6）佐々木勇人、瀬戸　崇志「サイバー攻撃対処における攻撃「キャンペーン」概念と「コスト賦課アプローチ」――近年の米国政府当局によるサイバー攻撃活動への対処事例の考察から」https://www.nids.mod.go.jp/publication/commentary/commentary346.html

[3] 本稿前編「能動的サイバー防御の実装に向けた残された論点（前編）～攻撃者のポートフォリオ分析の必要性～」注 1

[4] 軍事戦略において「勝利」の定義は明確に定まっていないが、スウェーデン国防大学のヤン・オングストロームとＪ・Ｊ・ワイデンの著書「軍事理論の教科書　戦争のダイナミクスを学ぶ（原題：Contemporary Military Theory: The Dynamics of War）」で紹介されている 4 つの観点／考え方から考察したもの（なお、各小見出しは便宜上筆者が付けたものである）

[5] 2025 年 7 月に米フォーダム大で開催されたカンファレンスにおいて、NSA と FBI の担当者は VoltTyphoon の攻撃キャンペーンは失敗に終わったと述べている。NSA: Volt Typhoon was ‘not successful’ at persisting in critical infrastructure　https://therecord.media/china-typhoon-hackers-nsa-fbi-response

[6] 2025/7/22 Microsoft, “Disrupting active exploitation of on-premises SharePoint vulnerabilities”, https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

[7] インテリジェンスの世界における実務上の慣習として「Need to Know」が重視されてきたところ、911 事件などにおける関係機関間の連携不足の課題に対するアプローチとして、「Need to Share」の必要性が指摘されるようになった。「Need to Know」と「Need to Share」の両立の難しさ、課題等については、小林良樹「なぜ、インテリジェンスは必要なのか」に詳しい（同書 195 ページほか）

[8] NIDS コメンタリー　第 319 号　2024 年 5 月 17 日（特集：「新領域の安全保障」 vol.3）佐々木勇人「サイバー脅威インテリジェンス活用のための「ドクトリン」の必要性について ―― 情報共有を巡る「市場の失敗」と「政府の失敗」を乗り越えるために」https://www.nids.mod.go.jp/publication/commentary/commentary319.html、国際安全保障学会 2024 年度年次大会　佐々木勇人「サイバー安全保障における民間主体のインテリジェンス機能と公私協働―米国の動向と日本の JPCERT/CC での実務の視点から―」

[9] Lennart Maschmeyer, “Secrecy in Strategy”,(収録先：edited by Robert Chesney and Max Smeets,Deter, “disrupt, or deceive: assessing cyber conflict as an intelligence contest”, Georgetown University Press） ほか、同じようなサイバー作戦のジレンマについて、Lennart Maschmeyer は、Subversion としてのサイバー作戦における「Subversive Trilemma」の理論を示している。The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations, https://direct.mit.edu/isec/article/46/2/51/107693/The-Subversive-Trilemma-Why-Cyber-Operations-Fall、Subversion From Covert Operations to Cyber Conflict, oxford university press,

[10] Ｊ・Ｃ・ワイリー（訳　奥山真司）「新装版　戦略論の原点」12 ページ。同じような指摘をサイバー作戦における「秘密性」との観点で示したものとして、前掲注 1 の Alexander Martin のコメントを挙げることができる。「すべてを完全に秘密裏に行う必要はない。つまり、ある程度、一部の能力は敵対勢力に晒されているし、民主主義国家として当然のことならが、国民に情報を提供し、情報に基づいた議論を促せるように、国民にも活動内容を伝えることで、どれほどの追加的リスクが生じるのはわかりません。これまで見てきたように、これらの機関が政治家や国民に十分な知識を提供し、理解を深め、豊かに議論しない限り、議論の質は非常に低くなる可能性があります」（前掲注 1　同書 77 ページ）

[11] 青井千由紀「戦略的コミュニケーションと国際政治　新しい安全保障政策の論理」（日本経済新聞出版、2022 年）45 ページ

PROFILE

佐々木　勇人

政策研究部サイバー安全保障研究室特任研究員（本務先：一般社団法人 JPCERT コーディネーションセンター　脅威アナリスト　早期警戒グループマネージャー　兼　政策担当部長）

専門分野：サイバーセキュリティ

防衛研究所企画部企画調整課
直　通：03-3260-3011
代　表：03-3268-3111（内線 29177）
防衛研究所 Web サイト：www.nids.mod.go.jp